Software Vulnerability Manager Release Notes

April 2018

Introduction

Software Vulnerability Manager reimagines how software is secured by closing the gap between IT Security and IT Operations by providing industry leading security research, risk assessment and remediation through Software Vulnerability Manager's key components:

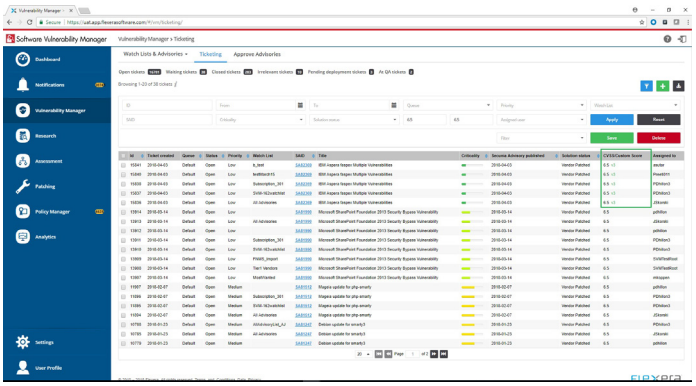
- **Research**: Keep up with the latest software vulnerability research and advisories from Secunia Research
- **Patching**: Remediate software vulnerabilities in third-party applications
- **Assessment**: Discover where software vulnerabilities are installed across your organization

New Features and Enhancements

The following table lists new features and enhancements for Software Vulnerability Manager. The Affected Module(s) column refers to the specific Software Vulnerability Manager module(s) affected by the new feature or enhancement.

Affected Module(s)	Feature or Enhancement Description	Reference Number
Assessment, Analytics, Online Help	A new Smart Groups feature has been added. Smart Groups allow you to organize your environment by defining dynamic groups of devices, products, or advisories based on your specific needs. These Smart Groups can be valuable in helping to focus on desired subsets of your environment (for example, server devices or critical advisories pertaining to a specific vendor). This Smart Group feature can also be especially beneficial in the prioritization of remediation efforts. For the online help reference, see: http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Smart_Groups.htm	SVM-228 and SVM-623
Patching, Settings, Online Help	Application Profiles are now referred to as Application Templates (the term “Profile” was replaced with “Template”). For the online help reference, see: http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Patching.htm In the Settings module under **Settings > Workflow Management > Rules**: ● “Patch available no customer profile” is now “Patch available, without template” ● “Patch available” is now “Patch available, with template” For the online help reference, see: http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Rules.htm	SVM-337

Affected Module(s)	Feature or Enhancement Description	Reference Number

All Modules	Support has been added to display CVSS 3.0 Scores. On May 18th, Flexera's Secunia Research will begin entering all new CVSS scores using the v3 standard. Once the CVSS 3.0 Scores are entered, they will appear in the User Interface, API, XML, email notifications, and PDF reports.
	
	In the User Interface
	
	The CVSS 3.0 score will be noted with a green "v3" after the score.
	
	 
	
	In the API
	
	API calls returning CVSS data will begin returning a second set of values for CVSSv3 so that you can programmatically differentiate between CVSSv2 and CVSSv3 scores. Once we change to providing CVSSv3 scores, the current `cvss_score` value will be blank and the value will appear as `cvss3_score`. The label `cvss_score` represents CVSSv2 (it was not renamed to avoid breaking existing scripts). New CVSS3 values will be represented as `cvss3_score`.
	
	`"cvss_info": {`
	`"cvss_overall_score": 7.4,`
	`"cvss_vector": "(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C)",`
	`"cvss_base_score": 10.0`
	`},`
	`"cvss_score": "10.0",`
	`"cvss_vector": "(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C)",`
	`"cvss3_info": {`
	`"cvss_overall_score": 4.6,`
	`"cvss_vector": "CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:U/RL:O/RC:C",`
	`"cvss_base_score": 5.3`
	`},`
	`"cvss3_score": "5.3",`
	`"cvss3_vector": "CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:U/RL:O/RC:C",`
	`"cvss_score_ui": "5.3",`
		SVM-387

Affected Module(s)	Feature or Enhancement Description	Reference Number
All Modules	**In the XML** A change to the schema is necessary to add specific values for CVSSv3 scores. As with the json API values above, we are adding a second cvss3 labeled value to distinguish v3 scores. Depending on how any scripts or processes consuming this data parse the information, **this has the potential to result in a breaking change.** <cvss_base_score>**10.0**</cvss_base_score> <cvss_overall_score>**7.4**</cvss_overall_score> <cvss_vector>**(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C)**</cvss_vector> <custom_cvss_overall_score>**7.2**</custom_cvss_overall_score> <custom_cvss_vector> **(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C/CDP:ND/TD:ND/CR:L/IR:ND/AR:ND)** </custom_cvss_vector> <cvss3_base_score>**5.3**</cvss3_base_score> <cvss3_overall_score>**4.6**</cvss3_overall_score> <cvss3_vector>**CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:U/RL:O/RC:C**</cvss3_vector> <custom_cvss3_overall_score>**4.7**</custom_cvss3_overall_score> <custom_cvss3_vector>**CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:U/RL:W/RC:C/CR:L/IR:X/A** **In Email Notifications** Emails will contain both v2 and v3 labels. The v3 value will be empty until we begin entry, at which time the v2 value will be empty. Highly critical Release Date 15/03/2018 Last Update 15/03/2018 Solution Status Vendor Patched SAID SA82054 CVSS 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C) CVSS3 5.3 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:U/RL:O/RC:C Impact System access Where From remote **In a PDF report** PDF reports containing CVSS values will show CVSS v2 (displayed as CVSS) or CVSS v3 (displayed as CVSS3) as appropriate. Criticality - Highly critical Impact System access Where From remote Solution Status Vendor Patched Secunia CVSS Scores Base: 10.0 , Overall: 7.4 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C) CVSS3 Base: 5.3 , Overall: 4.6 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:U/RL:O/RC:C CVE references CVE-2018-4920 | CVE-2018-4919 | For more on CVSS, see https://nvd.nist.gov/vuln-metrics/cvss	SVM-387, continued

Affected Module(s)	Feature or Enhancement Description	Reference Number
Research, Online Help	Under **Research > Advisory Database > Advisories**, the filter **CVE(s)** allows users to search for multiple advisories at the same time to determine which advisories apply to more than a single CVE for which users have interest. When entering multiple advisories, leave one space between entries (Example: CVE-2014-0224 CVE-2014-0160 CVE-2013-0169 CVE-2009-3555 CVE-2015-7575). For the online help reference, see: http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Advisories.htm	SVM-432
Notifications, Patching	The **Export to CSV** button is now present for all areas with filter buttons so that users can leverage filters to generate custom reports. The **Export to CSV** button was added to the following UI locations: • Notifications • Patching > Patch Library • Patching > Profiles • Patching > Packages • Patching > Deployment	SVM-465
Auditor, Settings, Online Help	The Auditor module has been moved to the Settings module and renamed as the subsection “Logs”. For the online help reference, see: http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Logs.htm	SVM-592
All Modules	The filters at the component level remain open after a user opens a panel even after they change views. This filter view only lasts for the current session or until the page is refreshed. To prevent an accidental deletion, a pop-up window appears when a user chooses to delete a saved filter.	SVM-608
Assessment, Online Help	To demonstrate the scanning performance of Software Vulnerability Manager as a Proof of Concept, run the Vulnerable Software Discovery Tool with immediate command line scan that will process scans fast, typically less than 1 minute: `SVMScan.exe -c --urgent-scan` For the online help reference, see: http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Vulnerable_Software_Discovery_Tool_Command_Line_Options.htm	SVM-618

Affected Module(s)	Feature or Enhancement Description	Reference Number
Online Help	Online help was clarified to provide rules for creating passwords. Create your password using the following password rules: • 8-200 characters • At least one lowercase letter • At least one uppercase letter • At least one digit Flexera recommends the following when creating passwords: • No common passwords • No personal details • No old passwords • Passwords created by a password generator For the online help reference, see: http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Logging_on_to_Software_Vulnerability_Manager.htm	SVM-624

Resolved Issues

No Resolved Issues were included with this release.

Product Feedback

Have a suggestion for how we can improve this product? Please come share direct feedback with the product team and vote on ideas submitted by other users in our Customer Community feedback page for Software Vulnerability Manager.

System Requirements

Software Vulnerability Manager's User Interface will resize and adapt when being used on different devices. You can access the system from anywhere using any device, such as a smartphone or tablet, running Internet Explorer 11 or higher, Chrome, Opera, Firefox, Safari and mobile browsers with an Internet connection capable of connecting to https://app.flexerasoftware.com.

Legal Information

Copyright Notice

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see https://www.flexera.com/producer/company/about/intellectual-property/. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.

Disclaimer

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. The provision of such information does not represent any commitment on the part of Flexera. Flexera makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Flexera shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The software described in this document is furnished by Flexera under a license agreement. The software may be used only in accordance with the terms of that license agreement. It is against the law to copy or use the software, except as specifically allowed in the license agreement. No part of this document may be reproduced or retransmitted in any form or by any means, whether electronically or mechanically, including, but not limited to: photocopying, recording, or information recording and retrieval systems, for any purpose other than the purchaser's personal use, without the express, prior, written permission of Flexera.